CLAIMS

What is claimed is:

1. A method of providing secure access to content comprising:

determining a secure medium identification (disk ID) from a secure medium including content;

sending a session key and the disk ID to a server;

requesting user authentication; and

if the user is successfully authenticated, receiving the session key from the server to enable reading of the content on the secure medium.

2. The method of claim 1, further comprising:

streaming encrypted content to an application.

3. The method of claim 2, further comprising;

the application using the session key returned by the server to decrypt the encrypted content, and display the content.

4. The method of claim 1, wherein the content is stored as encrypted content on the secure medium.

5. The method of claim 4, further comprising:

receiving a content decryption key from the server, in response to the disk ID and the user authentication.

6. The method of claim 5, wherein the content decryption key is determined based on the disk ID.

7. The method of claim 6, further comprising:

the application using the content decryption key and the session key returned by the server to decrypt the content received from the secure medium; and

playing the content.

8. The method of claim 1, further comprising a trusted device for accessing secure content:

reading the disk ID from the secure medium and generating a one-time session key; and

sending an encrypted copy of the disk ID and session key to the server.

9. The method of claim 8, wherein the disk ID and session key are encrypted using a symmetric key.

10. The method of claim 1, wherein the secure medium is selected from among the following: an optical disc, a flash memory, a hard drive, a magnetic drive, a memory stick, or another type of storage device.

11. The method of claim 1, wherein the content is digitally encoded music.

12. The method of claim 1, wherein user authentication comprises one or more of the following: a credit card, a debit card, electronic cash, a user-specific ID card.

13. The method of claim 1, wherein the user authentication comprises one or more of the following: a password, a user identification, a biometric identification.

14. The method of claim 1, wherein authenticating the user comprises:

determining if the disk ID is already associated with a user; and

if the disk ID is not yet associated with the user, associating the user authentication data with the disk ID.

15. The method of claim 15, further comprising:

if the disk ID is associated with a user, determining that the current user authentication matches the user associated with the disk ID, to authenticate the user.

16. The method of claim 15, further comprising:

if the user authentication does not match the user associated with the disk ID, refusing to return the session key, thereby preventing display of the content.

17. An apparatus comprising a secure device for accessing secure content coupled to a client system comprising:

a reader to read an identification (ID) and content from a secure medium;

an encryption logic to send the ID encrypted to a server;

an authentication logic to receive authentication from the server indicating approval to read the content of the secure medium;

the reader further to read the content; and the encryption logic further to encrypt the content prior to sending the content to an application.

18. The apparatus of claim 17, wherein the encryption logic uses a symmetric key to encrypt the ID.

19. The apparatus of claim 17, further comprising:

a session key generation logic to generate a one-time session key, the session key send with the ID to the server.

20. The apparatus of claim 17, further comprising an application on the client system comprising:

a user authentication interface to request a user authentication in response to a server request, and to send the data received from a user to the server;

a key logic to receive a decryption key from the server, if the user is successfully authenticated; and

a streaming decryption logic to receive data from the secure device and decrypt the data using the key received from the server, and play the data.

21. The apparatus of claim 20, wherein the decryption key is a session key and a content decryption key.

22. The apparatus of claim 17, further comprising a secure server coupled to the client system via a network, the secure server comprising:

a network interface to receive the ID and a session key from the secure device;

a user validation logic to request a user validation from the client system and determine whether the user has permission to access the secure medium identified by the ID; and

an encryption logic to return the session key and a content decryption key if the user has permission to access the secure medium.

23. The apparatus of claim 22, further comprising:

the encryption logic further to decrypt data received from the secure device using a symmetric key.

24. The apparatus of claim 22, further comprising:

an ID lookup to determine the content decryption key based on the ID.

25. A client system to securely access digital content on a secure medium, the client system comprising:

a secure device comprising:

a reader to read an ID and content from the secure medium;

an authentication logic to receive authentication from the server indicating approval to read the content of the secure medium; and

an encryption logic further to encrypt the content prior to sending the content to an application;

an application comprising:

a user authentication interface to request a user authentication in response to a server request, and to send the data received from a user to the server;

a key logic to receive a decryption key from the server, if the user is successfully authenticated; and

a streaming decryption logic to receive data from the secure device and decrypt the data using the key received from the server, and play the data.